

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Гандич Д.В.

29 февраля 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Гандич Дарья Владимировна
- студентка группы НБИбд-02-22
- Российский университет дружбы народов

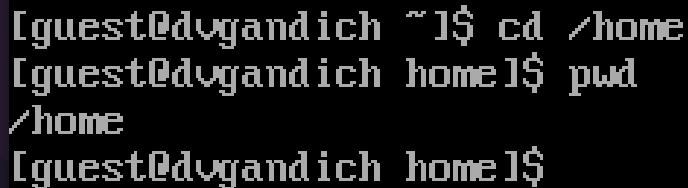
Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

1. Открываем VM, создаем учетную запись guest и задаем пароль.

```
dvgandich login: root
Password:
Last login: Tue Feb 27 16:26:17 on tty1
[root@dvgandich ~]# useradd guest
[root@dvgandich ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a (reversed) dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
[root@dvgandich ~]# _
```

Рис. 1: Создание учетной записи guest

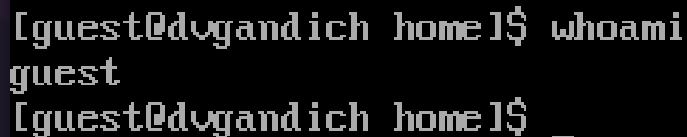
2. Определим директорию, в которой находимся с помощью команды pwd.

A terminal window with a black background and white text. The prompt is [guest@dvgandich ~]\$. The user enters 'cd /home'. The prompt changes to [guest@dvgandich home]\$. The user enters 'pwd'. The output is '/home'. The prompt returns to [guest@dvgandich home]\$.

```
[guest@dvgandich ~]$ cd /home
[guest@dvgandich home]$ pwd
/home
[guest@dvgandich home]$
```

Рис. 2: Определение директории pwd

3. Уточняем имя пользователя с помощью команды `whoami`.

A terminal window with a black background and white text. The prompt is [guest@dogandich home]\$. The command whoami is entered. The output is guest. The prompt changes to [guest@dogandich home]\$ _.

```
[guest@dogandich home]$ whoami
guest
[guest@dogandich home]$ _
```

Рис. 3: `whoami`

4. Уточним имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`.

Сравнивая вывод `id` с выводом команды `groups`, обнаружим, что группы, в которые входит пользователь, действительно одинаковые. Также, сравнивая вывод `id` с приглашением командной строки, обнаружим, что имя пользователя повторяется.

```
[guest@dvgandich home]$ id
uid=1000(guest) gid=1000(guest) groups=1000(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023
[guest@dvgandich home]$ groups
guest
[guest@dvgandich home]$
```

Рис. 4: Сравнение групп `id` и `groups`

5. Просмотрим файл `/etc/passwd` с помощью `cat /etc/passwd` и сравним данные `uid`, `gid` с результатами команд выше и выясним, что данные значения совпадают.

```
lguest@dygandich home1$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
sssd:x:997:993:User for sssd:/:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/:/usr/sbin/nologin
systemd-oom:x:990:990:systemd Userspace OOM Killer:/:/usr/sbin/nologin
setroubleshoot:x:989:989:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
cockpit-ws:x:988:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:987:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:986:986:chrony system user:/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
guest:x:1000:1000:~/home/guest:/bin/bash
lguest@dygandich home1$ _
```

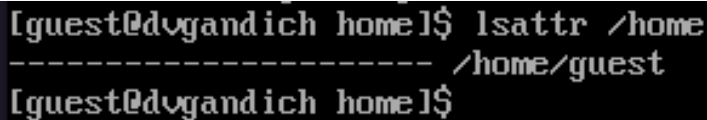
Рис. 5: Сравнение значений `uid` и `gid`

6. Определим существующие в системе директории командой `ls -l /home/`. Нам удалось получить список поддиректорий. У каждой из них установлены права на чтение, запись и выполнение только для самого пользователя.

```
[guest@dvgandich home]$ ls -l /home/  
total 0  
drwx-----. 2 guest guest 62 Feb 29 13:02 guest  
[guest@dvgandich home]$ _
```

Рис. 6: Существующие директории и доступные права

7. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home`. Нам удалось увидеть расширенные атрибуты директории, но не удалось увидеть расширенные атрибуты директорий других пользователей.



```
[guest@dvgandich home]$ lsattr /home
----- /home/guest
[guest@dvgandich home]$
```

Рис. 7: `lsattr /home`

8. Создаем в домашней директории поддиректорию dir1. Определяем командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.

```
[guest@dogandich ~]$ mkdir dir1
[guest@dogandich ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 29 14:20 dir1
[guest@dogandich ~]$ lsattr
----- ./dir1
[guest@dogandich ~]$
```

Рис. 8: Создание поддиректории

9. Снимите с директории dir1 все атрибуты командой `chmod 000 dir1` и проверьте с её помощью правильность выполнения команды `ls -l`.

```
[guest@dogandich ~]$ chmod 000 dir1
[guest@dogandich ~]$ ls -l
total 0
d----- . 2 guest guest 6 Feb 29 14:20 dir1
[guest@dogandich ~]$ _
```

Рис. 9: Снятие всех атрибутов

10. Попытаемся создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1. Мы получим отказ от выполнения, так как шагом ранее сняли все атрибуты с директории. Проверим, действительно ли файл не создавался, с помощью команды ls -l /home/guest/dir1.

```
[guest@dvchandich ~]$ chmod 000 dir1
[guest@dvchandich ~]$ ls -l
total 0
d----- . 2 guest guest 6 Feb 29 14:20 dir1
[guest@dvchandich ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
[guest@dvchandich ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@dvchandich ~]$ chmod 777 dir1
[guest@dvchandich ~]$ ls -l /home/guest/dir1
total 0
[guest@dvchandich ~]$
```

Рис. 10: Создание файла

11. Заполняем таблицу 2.1 “Установленные права и разрешенные действия”.

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименовывание файла	Смена атрибутов файла
d----- (000)	0	-	-	-	-	-	-	-	-
d--x----- (100)	0	-	-	-	-	+	-	-	+
d-w----- (200)	0	-	-	-	-	-	-	-	-
d-wx----- (300)	0	+	+	-	-	+	-	+	+
dx----- (400)	0	-	-	-	-	-	+	-	-
dx-x----- (500)	0	-	-	-	-	+	+	-	+
dxw----- (600)	0	-	-	-	-	-	+	-	-
dxwx----- (700)	0	+	+	-	-	+	+	+	+
d----- (000)	--x----- (100)	-	-	-	-	-	-	-	-
d--x----- (100)	--x----- (100)	-	-	-	-	+	-	-	+
d-w----- (200)	--x----- (100)	-	-	-	-	-	-	-	-
d-wx----- (300)	--x----- (100)	+	+	-	-	+	-	+	+
dx----- (400)	--x----- (100)	-	-	-	-	-	+	-	-
dx-x----- (500)	--x----- (100)	-	-	-	-	+	+	-	+
dxw----- (600)	--x----- (100)	-	-	-	-	-	+	-	-
dxwx----- (700)	--x----- (100)	+	+	-	-	+	+	+	+
d----- (000)	-w----- (200)	-	-	-	-	-	-	-	-
d--x----- (100)	-w----- (200)	-	-	+	-	+	-	-	+
d-w----- (200)	-w----- (200)	-	-	-	-	-	-	-	-
d-wx----- (300)	-w----- (200)	+	+	+	-	+	-	+	+
dx----- (400)	-w----- (200)	-	-	-	-	-	+	-	-
dx-x----- (500)	-w----- (200)	-	-	+	-	+	+	-	+
dxw----- (600)	-w----- (200)	-	-	-	-	-	+	-	-
dxwx----- (700)	-w----- (200)	+	+	+	-	+	+	+	+

Рис. 11: Таблица “УПирД”

d----- (000)	-wx----- (300)	-	-	-	-	-	-	-	-
d-x----- (100)	-wx----- (300)	-	-	+	-	+	-	-	+
d-w----- (200)	-wx----- (300)	-	-	-	-	-	-	-	-
d-wx----- (300)	-wx----- (300)	+	+	+	-	+	-	+	+
dx----- (400)	-wx----- (300)	-	-	-	-	-	+	-	-
dx-x----- (500)	-wx----- (300)	-	-	+	-	+	+	-	+
dxw----- (600)	-wx----- (300)	-	-	-	-	-	+	-	-
dxwx----- (700)	-wx----- (300)	+	+	+	-	+	+	+	+
d----- (000)	f----- (400)	-	-	-	-	-	-	-	-
d-x----- (100)	f----- (400)	-	-	-	+	+	-	-	+
d-w----- (200)	f----- (400)	-	-	-	-	-	-	-	-
d-wx----- (300)	f----- (400)	+	+	-	+	+	-	+	+
dx----- (400)	f----- (400)	-	-	-	-	-	+	-	-
dx-x----- (500)	f----- (400)	-	-	-	+	+	+	-	+
dxw----- (600)	f----- (400)	-	-	-	-	-	+	-	-
dxwx----- (700)	f----- (400)	+	+	-	+	+	+	+	+
d----- (000)	f-x----- (500)	-	-	-	-	-	-	-	-
d-x----- (100)	f-x----- (500)	-	-	-	+	+	-	-	+
d-w----- (200)	f-x----- (500)	-	-	-	-	-	-	-	-
d-wx----- (300)	f-x----- (500)	+	+	-	+	+	-	+	+
dx----- (400)	f-x----- (500)	-	-	-	-	-	+	-	-
dx-x----- (500)	f-x----- (500)	-	-	-	+	+	+	-	+
dxw----- (600)	f-x----- (500)	-	-	-	-	-	+	-	-
dxwx----- (700)	f-x----- (500)	+	+	-	+	+	+	+	+

Рис. 12: Таблица “УПиРД”

d----- (000)	rw----- (600)	-	-	-	-	-	-	-	-
d-x----- (100)	rw----- (600)	-	-	+	+	+	-	-	+
d-w----- (200)	rw----- (600)	-	-	-	-	-	-	-	-
d-wx----- (300)	rw----- (600)	+	+	+	+	+	-	+	+
dx----- (400)	rw----- (600)	-	-	-	-	-	+	-	-
dx-x----- (500)	rw----- (600)	-	-	+	+	+	+	-	+
dx-w----- (600)	rw----- (600)	-	-	-	-	-	+	-	-
dxwx----- (700)	rw----- (600)	+	+	+	+	+	+	+	+
d----- (000)	rwX----- (700)	-	-	-	-	-	-	-	-
d-x----- (100)	rwX----- (700)	-	-	+	+	+	-	-	+
d-w----- (200)	rwX----- (700)	-	-	-	-	-	-	-	-
d-wx----- (300)	rwX----- (700)	+	+	+	+	+	-	+	+
dx----- (400)	rwX----- (700)	-	-	-	-	-	+	-	-
dx-x----- (500)	rwX----- (700)	-	-	+	+	+	+	-	+
dx-w----- (600)	rwX----- (700)	-	-	-	-	-	+	-	-
dxwx----- (700)	rwX----- (700)	+	+	+	+	+	+	+	+

Рис. 13: Таблица “УПирД”

12. Заполняем таблицу 2.2 “Минимальные права для совершения операций”.

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)
Чтение файла	d--x----- (100)	r----- (400)
Запись в файл	d--x----- (100)	-w----- (200)
Переименовывание файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

Рис. 14: Таблица “МПДСО”

- Получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

мы молодцы! :::